

Public Information Officers Database (PIOneer) – Privacy Impact Assessment

PIA Approval Date: February 4, 2009

System Overview

Public Information Officer (PIOneer), is a web-based application, which will allow the Public Information Officers (PIO) and Criminal Investigation's (CI) Headquarters staff to collect, monitor, and report incoming and outgoing media correspondences, related CI investigations and associated legal actions. This will increase the PIO's effectiveness in their communication and outreach to the media and public outlets. The PIONeer application synchronizes investigation data with Criminal Investigation Management Information System (CIMIS).

Systems of Records Notice (SORN):

- Treasury/IRS 34.037, IRS Audit Trail and Security Records System
- Treasury/IRS 46.003, Criminal Investigation Management Information System (CIMIS)

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer: Identity of the subject of an investigation. Data includes:

- Name
- Taxpayer Identification Number (TIN)
- Date of Birth (DOB)
- Address
- Aliases
- Occupation
- Industry

B. Employee:

- Name
- Post of duty
- Phone/email contact information for the Lead and Secondary case agent

C. Audit Trail Information (including employee log-in info):

- The system records all data queries and data changes made, recording the date/time of the access/change and user's network login
- Web service logs track view page requests to the server, and the server's responses

D. Other (Describe):

- Data about criminal investigations in progress, including information about the alleged violation, violation type (statute), CI program areas, investigation status, assigned Assistant United States Attorney (AUSA) or Department of Justice (DOJ) attorney name, address, phone, name of the judge, address of courthouse links to documents about investigative actions
- Number Optional feature: Records of media contacts, including name, title, organization, address, phone/fax/email, contact date, topic of contact #
- Records of outreach activities, including organization name, type, date/time of event, event address, organization contact name, phone, email, fax, date of

request, assigned speaker name/title, office, event history, links to documents about the outreach event

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS: The following information is downloaded nightly from the Criminal Investigation Management Information System (CIMIS):

- Data about the Subject of the investigation
- Data about criminal investigations in progress
- Data about the primary and secondary Special Agents assigned to the investigation, such as CI Field office location

PIOneer Application users manually enter data provided by contacts for:

- Records of outreach events
- Records of contact with members of the media or other public information contacts
- Data about attorneys and judges involved in legal actions

3. Is each data item required for the business purpose of the system? Explain.

Yes. All data is required for the business purposes and operations of the system. The business purpose of the system is to track legal actions and store publicity information related to criminal investigations. The system also stores data about community outreach events managed by the Public Information Officer as part of his/her official duties.

4. How will each data item be verified for accuracy, timeliness, and completeness?

Data provided by CIMIS is verified by CIMIS users and managers. The CIMIS data extract is scheduled to be provided on a nightly basis, so that investigations data is current as of the previous business day. Data entered by PIO users is manually reviewed for accuracy, timeliness and completeness throughout the investigation lifecycle.

5. Is there another source for the data? Explain how that source is or is not used.

No. There is no other source for the data not previously identified in Question 2.

6. Generally, how will data be retrieved by the user?

Authorized users will use a search function in the PIOneer application to retrieve data, based on need-to-know access rights and permissions.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?

Yes. Data can be retrieved using the following personal identifiers:

- Name of subject (person or business)
- Name of agent

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

The following types of users have access to the system:

- System Administrator – permission to troubleshoot problems with the application, and to add users to the system’s groups and permissions table.
- Database Administrator – full access to the database server to administer the PIONEER database.
- Application Administrator (Contractor) – temporary authorized system administrator-level access on the Web servers to assist in trouble shooting problems with the application.
- PIO – Public Information Officers have permissions within their field office to read/write information and run reports.
- Field Office Managers have permissions within their field office to view investigative data and calendar events and add miscellaneous events to the calendar.
- Headquarters Communications and Education Staff – permissions to read/write headquarters information, view nationwide events, and run reports within their scope.
- Headquarters Managers and analysts – permissions to view information in order to perform analysis within their scope.

9. How is access to the data by a user determined and by whom?

All user accounts are managed by the OL5081 process and authorized by the business owner. The business owner determines which users will have access and follows IRS CI procedures to instruct the System Administrators and IRS CI DBA to give the appropriate access on the system.

All contractors are required to have a High-Risk Background Investigation.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.

The following information is downloaded nightly from the Criminal Investigation Management Information System (CIMIS):

- Data about the Subject of the investigation
- Data about criminal investigations in progress
- Data about the Primary and secondary Special Agents assigned to the investigation, such as CI Field office location

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

Yes. CIMIS has a current Approval to Operate (ATO) and an approved Privacy Impact Assessment.

System
CIMIS

C&A
5/8/09

PIA
Yes

12. Will other agencies provide, receive, or share data in any form with this system?

No other agencies will provide, receive, or share data in any form with the system.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

Records are maintained, administered and disposed of in accordance per IRM 1.15.30, Records Management, Records Control Schedule for Criminal Investigation, January 1, 2003. PIONEER retains the audit logs in compliance to IRM 10.8.3, Audit Logging Security Standards.

14. Will this system use technology in a new way?

No. This system will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.

Yes. The business purpose of this information is to enable the Public Information Officer to accurately respond to inquiries from the media, and to contact journalists or organizations who have made inquiries. The location of legal actions related to an investigation determines the location of media outlets that may contain publicity about the investigation. Tracking the publicity is a business purpose of PIONEER.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.

No. PIONEER does not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?

No. PIONEER does not allow IRS to treat taxpayers, employees, or others differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

Not applicable. PIONEER does not make any determinations about affected parties.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

No. PIONEER is only accessed by CI employees and contractors having hi-level BI so it is not an externally available web-based application. Standard session cookies and network login are used for the purpose of user session management; however, persistent cookies are not used by this system.

[View other PIAs on IRS.gov](#)